12

The geometry of numbers

We now prove some of the basic results of the geometry of numbers, limiting ourselves to those which help one to handle linear inequalities. A fuller exposition (such as that given by Cassels [12]) would be both more general and more precise: more general in that ordinary distances are replaced by distances in a metric, and more precise in that attention is paid to constants depending on n (the number of dimensions). Such constants are of no importance for the purpose we have in mind.

A lattice Λ, in n-dimensional space, is the set of all (real) points

$$\mathbf{x} = (x_1, \ldots, x_n)$$

given by n linear forms in n variables $u_1, \ldots, u_n$ which take integral values:

$$\begin{aligned} x_1 &= \lambda_{11}u_1 + \cdots + \lambda_{1n}u_n, \\ &\vdots \\ x_n &= \lambda_{n1}u_1 + \cdots + \lambda_{nn}u_n, \end{aligned}$$

or $\mathbf{x} = \Lambda\mathbf{u}$ in matrix notation. The coefficients λ_{ij} are real numbers with $\det \lambda_{ij} \neq 0$. A linear integral substitution of determinant 1 (unimodular substitution) applied to the variables $u_1, \ldots, u_n$ does not change the lattice. The points of the lattice can also be represented by

$$\mathbf{x} = u_1\mathbf{x}^{(1)} + \cdots + u_n\mathbf{x}^{(n)},$$

where $\mathbf{x}^{(j)} = (\lambda_{1j}, \ldots, \lambda_{nj})$ for $j = 1, \ldots, n$. The points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ constitute a *basis* for the lattice, and the change of variable just mentioned corresponds to a change of basis.

We define the *determinant* $d(\Lambda)$ of Λ by

$$d(\Lambda) = |\det \lambda_{ij}|;$$

this is a positive number, unaffected by unimodular changes of variable. The density of the lattice (in an obvious sense) is $1/d(\Lambda)$. The determinant of the coordinates of any set of n lattice points is an integral multiple of $d(\Lambda)$. We shall usually suppose $d(\Lambda) = 1$ for convenience.

An *affine transformation* of space is a (homogeneous) linear transformation, with real coefficients and determinant $\neq 0$, from $x_1, \ldots, x_n$ to $y_1, \ldots, y_n$. This maps the lattice Λ in x-space into a lattice M in y-space, and if the affine transformation has determinant 1 then $d(\Lambda) = d(\mathsf{M})$.

Lemma 12.1. *Any ellipsoid with centre at the origin O and volume $>$ 2^n contains a point, other than O, of every lattice of determinant* 1.

Proof. It suffices to prove the result for a sphere, since an ellipsoid can be transformed into a sphere by an affine transformation of space of determinant 1. Let ρ be the radius of the sphere. Since $d(\Lambda) = 1$, the number of points of Λ in a cube of large side X is asymptotic to X^n as $X \to \infty$. If we place a sphere of radius $\frac{1}{2}\rho$ (and therefore of volume $V > 1$) with its centre at each of these lattice points, their total volume is asymptotically VX^n. They are all contained in a cube of side $X+\rho$. For large X we have $VX^n > (X+\rho)^n$, so two of the spheres must overlap. Thus there are two distinct points of Λ with distance apart less than ρ, and so there is a point of Λ, other than O, within a distance ρ of O. $\square$

Note. This result, with the ellipsoid replaced by any convex body which has central symmetry about O, is Minkowski's first fundamental theorem. The proof is essentially the same.

The *successive minima* of a lattice Λ are defined as follows. Let R_1 be the least distance of any point of Λ, other than O, from O, and let $\mathbf{x}^{(1)}$ be a point of Λ at this distance. Denoting by $|\mathbf{x}|$ the distance of a point $\mathbf{x}$ from O, we have $|\mathbf{x}^{(1)}| = R_1$. Let R_2 be the least distance from O of any point which is not on the line $\langle O, \mathbf{x}^{(1)} \rangle$, and let $\mathbf{x}^{(2)}$ be such a point with $|\mathbf{x}^{(2)}| = R_2$. Let R_3 be the least distance from O of any point of Λ which is not in the plane $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \rangle$, and so on. We obtain numbers $R_1, \ldots, R_n$ and linearly independent points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$, such that

$$0 < R_1 \leq R_2 \leq \cdots \leq R_n, \qquad |\mathbf{x}^{(\nu)}| = R_\nu.$$

The points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ can possibly be chosen in more than one way, but it is easily seen that this does not affect the uniqueness of the numbers $R_1, \ldots, R_n$. These numbers are the successive minima of Λ, and

$\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ is a set of minimal points of Λ. These points do not necessarily constitute a basis, though this happens to be the case when $n = 2$.

Lemma 12.2. *If $d(\Lambda) = 1$, we have*

$$1 \leq R_1 R_2 \cdots R_n \leq 2^n / J_n, \tag{12.1}$$

where J_n denotes the volume of a sphere of radius 1 *in n dimensions.*

Proof. We can rotate the n-dimensional space about O until

$$\begin{aligned}
\mathbf{x}^{(1)} &= (x_1^{(1)}, 0, 0, \ldots, 0), \\
\mathbf{x}^{(2)} &= (x_1^{(2)}, x_2^{(2)}, 0, \ldots, 0), \\
&\vdots \\
\mathbf{x}^{(n)} &= (x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, \ldots, x_n^{(n)}).
\end{aligned}$$

Since the determinant of these n points is an integral multiple of $d(\Lambda) = 1$ and they are linearly independent, we have

$$|x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}| \geq 1.$$

Since $R_\nu = |\mathbf{x}^{(\nu)}| \geq |x_\nu^{(\nu)}|$, we obtain $R_1 R_2 \cdots R_n \geq 1$.

To obtain an upper bound for $R_1 R_2 \cdots R_n$, we consider the ellipsoid

$$\frac{x_1^2}{R_1^2} + \cdots + \frac{x_n^2}{R_n^2} < 1.$$

This contains no point of Λ other than O. For suppose a point $\mathbf{x}$ of Λ is linearly dependent on $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\nu)}$ but not on $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\nu-1)}$, where $1 \leq \nu \leq n$. Then $|\mathbf{x}| \geq R_\nu$ by the definition of R_ν. Also $x_{\nu+1} = 0, \ldots, x_n = 0$; whence

$$\frac{x_1^2}{R_1^2} + \cdots + \frac{x_n^2}{R_n^2} \geq \frac{x_1^2 + \cdots + x_\nu^2}{R_\nu^2} \geq 1.$$

Thus $\mathbf{x}$ is not in the ellipsoid. It follows from Lemma 12.1 that the volume of the ellipsoid is $\leq 2^n$. This volume is $(R_1 R_2 \cdots R_n) J_n$, and the desired inequality follows. □

Note. Lemma 12.2, and the definitions concerning successive minima, again extend to an arbitrary convex body with center O. In this more general form, Lemma 12.2 is Minkowski's second fundamental theorem; but its proof is then considerably more difficult. Note that Lemma 12.2 implies $J_n R_1^n \leq 2^n$, which is the result of Lemma 12.1.

We introduce temporarily the notation $A \asymp B$ to mean both $A \ll B$ and $A \gg B$; in other words, to indicate that A/B is bounded both above and below by numbers depending only on n.

Lemma 12.3. *After an appropriate rotation of space, any lattice of determinant* 1 *has a basis* $\mathbf{X}^{(1)}, \ldots, \mathbf{X}^{(n)}$ *of the form*

$$\mathbf{X}^{(1)} = (X_1^{(1)}, 0, 0, \ldots, 0), \quad \mathbf{X}^{(2)} = (X_1^{(2)}, X_2^{(2)}, 0, \ldots, 0), \quad \ldots$$

where

$$|\mathbf{X}^{(\nu)}| \asymp R_\nu \qquad \text{and} \qquad |X_\nu^{(\nu)}| \asymp R_\nu, \tag{12.2}$$

for $\nu = 1, \ldots, n$.

Proof. We obtain the basis points by a process of adaptation from the minimal points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}_n^{(n)}$ in the proof of Lemma 12.2. We take $\mathbf{X}^{(1)}$ to be $\mathbf{x}^{(1)}$. We take $\mathbf{X}^{(2)}$ to be a point of Λ in the plane $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}\rangle$ which, together with $\mathbf{X}^{(1)}$, generates integrally all points of Λ in that plane; the existence of such a point is geometrically intuitive. It is arbitrary to the extent of any added multiple of $\mathbf{x}^{(1)}$. Since $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ generate rationally (though perhaps not integrally) all points of Λ in the plane $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}\rangle$, we have

$$N\mathbf{X}^{(2)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)}$$

for certain integers $N > 0$, u_1, u_2. Since $\mathbf{x}^{(2)}$ is an integral linear combination of $\mathbf{X}^{(2)}$ and $\mathbf{X}^{(1)} = \mathbf{x}^{(1)}$, we must have $u_2 = 1$. By adding to $\mathbf{X}^{(2)}$ a suitable integral multiple of $\mathbf{x}^{(1)}$, we can suppose that $|u_1| \le \frac{1}{2}N$. Then

$$|\mathbf{X}^{(2)}| \le \left|\frac{u_1}{N}\right| |\mathbf{x}^{(1)}| + \frac{1}{N}|\mathbf{x}^{(2)}| \le \frac{1}{2}R_1 + R_2 \le \frac{3}{2}R_2.$$

Next we take $\mathbf{X}^{(3)}$ to be a point of Λ in the space $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \mathbf{x}^{(3)}\rangle$ which, together with $\mathbf{X}^{(1)}$, $\mathbf{X}^{(2)}$, generates integrally all points of Λ in that space; the choice of $\mathbf{X}^{(3)}$ is arbitrary to the extent of added multiples of $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$, and *a fortiori* of added multiples of $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$. For the same reason as before, we have

$$N\mathbf{X}^{(3)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)} + u_3\mathbf{x}^{(3)}$$

for certain integers $N > 0$, u_1, u_2, u_3. This time we cannot conclude that $u_3 = 1$, but we can conclude that u_3 divides N, for $\mathbf{x}^{(3)}$ is expressible as

$$\mathbf{x}^{(3)} = v_1\mathbf{X}^{(1)} + v_2\mathbf{X}^{(2)} + v_3\mathbf{X}^{(3)},$$

and we must have $N = u_3v_3$. As before, we can ensure that $|u_1| \le \frac{1}{2}N$ and $|u_2| \le \frac{1}{2}N$. Hence

$$|\mathbf{X}^{(3)}| \le \frac{1}{2}|\mathbf{x}^{(1)}| + \frac{1}{2}|\mathbf{x}^{(2)}| + |\mathbf{x}^{(3)}| \le \frac{1}{2}R_1 + \frac{1}{2}R_2 + R_3 \le 2R_3.$$

Continuing in this way, we get an integral basis for Λ satisfying

$$|\mathbf{X}^{(\nu)}| \le \frac{\nu+1}{2}R_\nu \ll R_\nu, \quad (1 \le \nu \le n).$$

Since $\mathbf{X}^{(\nu)}$ is a linear combination of $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\nu)}$, its last $n-\nu$ coordinates are 0. We have

$$|X_\nu^{(\nu)}| \le |\mathbf{X}^{(\nu)}| \ll R_\nu,$$

so we have both the upper bounds in (12.2). The lower bounds follow from a comparison of determinants, together with (12.1). Since $d(\Lambda) = 1$, we have

$$|X_1^{(1)} \cdots X_n^{(n)}| = 1,$$

whence

$$R_1 \cdots R_{\nu-1}|X_\nu^{(\nu)}|R_{\nu+1} \cdots R_n \gg 1,$$

and the right-hand half of (12.1) gives

$$|X_\nu^{(\nu)}| \gg R_\nu.$$

Hence, *a fortiori*, $|\mathbf{X}^{(\nu)}| \gg R_\nu$. Alternatively, the last inequality would follow from the definition of the numbers $R_1, \ldots, R_n$. □

Note. The integral basis found in Lemma 12.3 can be further 'normalized', if desired. By adding suitable multiples of $\mathbf{X}^{(1)}, \ldots, \mathbf{X}^{(\nu-1)}$ to $\mathbf{X}^{(\nu)}$ we can ensure that

$$|X_\mu^{(\nu)}| \le \frac{1}{2}|X_\mu^{(\mu)}|$$

for all μ, ν with $\mu < \nu$.

Lemma 12.4. *Suppose $d(\Lambda) = 1$. Let $N(R)$ denote the number of $\mathbf{x}$ of Λ (including the origin) with $|\mathbf{x}| \le R$. Then $N(R) = 1$ if $R < R_1$, and if $R_\nu \le R < R_{\nu+1}$ then*

$$N(R) \asymp \frac{R^\nu}{R_1R_2\cdots R_\nu}.$$

Note. If $\nu = n$ then R_{n+1} is to be omitted from the condition $R_\nu \le R < R_{\nu+1}$.

Proof. The first result stated is obvious; the only point of Λ with $|\mathbf{x}| < R_1$ is the origin. To obtain the lower bound for $N(R)$ in the general case, we consider all points of the form

$$\mathbf{x} = u_1\mathbf{X}^{(1)} + \cdots + u_\nu\mathbf{X}^{(\nu)},$$

where $u_1, \ldots, u_\nu$ take all integral values satisfying

$$|u_j| \le \frac{1}{\nu}\frac{R}{|\mathbf{X}^{(j)}|}, \quad (1 \le j \le \nu).$$

All these points have $|\mathbf{x}| \le R$. The number of choices for $u_1, \ldots, u_\nu$ (since zero values are allowed) is

$$\gg \prod_{j=1}^{\nu} \frac{R}{|\mathbf{X}^{(j)}|} \gg \frac{R^\nu}{R_1R_2\cdots R_\nu},$$

by Lemma 12.3.

For the upper bound, we note first that all points $\mathbf{x}$ of Λ with $|\mathbf{x}| \le R$ must be linearly dependent on $\mathbf{X}^{(1)}, \ldots \mathbf{X}^{(\nu)}$, since $R < R_{\nu+1}$. Hence they are representable as

$$\mathbf{x} = v_1\mathbf{X}^{(1)} + \cdots + v_\nu\mathbf{X}^{(\nu)}$$

with integers $v_1, \ldots, v_\nu$. For this point, we have

$$\begin{aligned} x_\nu &= v_\nu X_\nu^{(\nu)}, \\ x_{\nu-1} &= v_\nu X_{\nu-1}^{(\nu)} + v_{\nu-1}X_{\nu-1}^{(\nu-1)}, \end{aligned}$$

and so on. Since each coordinate of $\mathbf{x}$ has absolute value $\le R$, the number of possibilities for v_ν is $\ll R/|X_\nu^{(\nu)}|$, and when v_ν is chosen, the number of possibilities for $v_{\nu-1}$ is $\ll R/|X_{\nu-1}^{(\nu-1)}|$, and so on. (Note that all these numbers are $\gg 1$, otherwise the argument would be fallacious.) Hence, using Lemma 12.3 again, we conclude that the number of points $\mathbf{x}$ is

$$\ll \frac{R^\nu}{|X_1^{(1)}|\cdots|X_\nu^{(\nu)}|} \ll \frac{R^\nu}{R_1R_2\cdots R_\nu}.$$

□

Note. The general meaning of Lemma 12.4 is that, for the purpose of counting the lattice points in a sphere (or other convex body of fixed shape), every lattice behaves like the rectangular lattice generated by

$$(R_1, 0, 0, \ldots, 0), (0, R_2, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, R_n),$$

up to a constant depending only on n. Thus for many purposes we can adequately describe a lattice by means of the n positive numbers $R_1, \ldots, R_n$.

A lattice Λ in x space and a lattice M in y space will be said to be *adjoint*, or *polar* if their bases can be chosen so that

$$\Lambda^T \mathsf{M} = I,$$

where T denotes the transpose of a matrix. If the lattices are given by $\mathbf{x} = \Lambda\mathbf{u}$ and $\mathbf{y} = \mathsf{M}\mathbf{v}$ respectively, where $\mathbf{u}$ and $\mathbf{v}$ are integral vectors the condition means that

$$x_1 y_1 + \cdots + x_n y_n = u_1 v_1 + \cdots + u_n v_n \tag{12.3}$$

identically. Note that $d(\Lambda)d(\mathsf{M}) = 1$. The relation between Λ and M is symmetrical. But the relation is not invariant under arbitrary linear transformations of the x space and the y space; if $\mathbf{x} = A\mathbf{x}'$ and $\mathbf{y} = B\mathbf{y}'$, the relation will only be preserved if $A^T B = I$.

Lemma 12.5. (Mahler) *If Λ, M are adjoint lattices of determinant 1, with successive minima $R_1, \ldots, R_n$ and $S_1, \ldots S_n$, respectively, then*

$$R_1 \asymp \frac{1}{S_n},\ R_2 \asymp \frac{1}{S_{n-1}}, \ldots, R_n \asymp \frac{1}{S_1}.$$

Proof. Let $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ be the minimal points for Λ (not necessarily a basis) and let $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(n)}$ be minimal points for M. The identity (12.3) implies that for any points $\mathbf{x}, \mathbf{y}$ of Λ, M either $\mathbf{x}$ is perpendicular[1] to $\mathbf{y}$ or

$$|x_1 y_1 + \cdots + x_n y_n| \geq 1,$$

whence $|\mathbf{x}||\mathbf{y}| \geq 1$. The $\mathbf{y}$ that are perpendicular to every $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\nu)}$ form an $(n-\nu)$-dimensional linear space. It cannot contain more than $n - \nu$ linearly independent points of y space, and so cannot contain all of $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(n-\nu+1)}$. Hence there exist $r \leq \nu$ and $s \leq n - \nu + 1$ such that $|\mathbf{x}^{(r)}||\mathbf{y}^{(s)}| \geq 1$. Now $|\mathbf{x}^{(r)}| \leq R_\nu$ and $|\mathbf{y}^{(s)}| \leq S_{n-\nu+1}$. It follows that

$$R_\nu S_{n-\nu+1} \geq 1, \quad (1 \leq \nu \leq n). \tag{12.4}$$

An inequality in the opposite direction follows by comparing products.

[1] We mean, of course, that the vector from O to $\mathbf{x}$ is perpendicular to that from O to $\mathbf{y}$.

Since

$$R_1 \cdots R_n S_1 \cdots S_n \le \left(\frac{2^n}{J_n}\right)^2$$

by Lemma 12.2, it follows from (12.4) that

$$R_\mu S_{n-\mu+1} \ll \left(\frac{2^n}{J_n}\right)^2, \quad (1 \le \mu \le n).$$

This proves Lemma 12.5. □

Note. The condition $d(\Lambda) = 1$ in Lemma 12.5 is unnecessary, but involves no loss of generality. When Lemma 12.5 is extended to the successive minima relative to any convex body (with central symmetry about the origin), it is necessary to use a body in x space and a body in y space which are polar to one another with respect to the unit sphere.

There is a particular type of lattice in $2n$-dimensional space which is essentially self-adjoint. Let Λ denote the $2n$-dimensional lattice given by

$$\begin{aligned} ax_1 &= u_1, \\ &\vdots \\ ax_n &= u_n, \\ a^{-1}x_{n+1} &= \gamma_{11}u_1 + \cdots + \gamma_{1n}u_n + u_{n+1}, \\ &\vdots \\ a^{-1}x_{2n} &= \gamma_{n1}u_1 + \cdots + \gamma_{nn}u_n + u_{2n}, \end{aligned}$$

where $a \ne 0$ and the numbers γ_{ij} are real. This has a matrix of the form

$$\Lambda = \begin{pmatrix} a^{-1}I_n & 0 \\ a\gamma & aI_n \end{pmatrix}.$$

The adjoint lattice has the matrix

$$\mathsf{M} = (\Lambda^T)^{-1} = \begin{pmatrix} aI_n & -a\gamma^T \\ 0 & a^{-1}I_n \end{pmatrix}.$$

If $\gamma^T = \gamma$, that is if

$$\gamma_{ij} = \gamma_{ji} \quad \text{for all } i, j, \tag{12.5}$$

then the lattice M can be transformed into the lattice Λ by (i) changing the signs of $v_{n+1}, \dots, v_{2n}$, (ii) changing the signs of $y_{n+1}, \dots, y_{2n}$, (iii) interchanging $v_1, \dots, v_n$ and $v_{n+1}, \dots, v_{2n}$, (iv) interchanging $y_1, \dots, y_n$ and $y_{n+1}, \dots, y_{2n}$.

Hence, subject to (12.5), the successive minima of M are the same as those of Λ. By the last lemma, it follows that

$$R_1 R_{2n} \asymp 1, \ldots, R_n R_{n+1} \asymp 1.$$

In particular, we have

$$R_n \ll 1 \ll R_{n+1}.$$

We can now prove the main result needed for the later work on cubic forms.

Lemma 12.6. *Let $L_1, \ldots, L_n$ be linear forms:*

$$L_i = \gamma_{i1} u_1 + \cdots + \gamma_{in} u_n, \quad (1 \le i \le n),$$

satisfying the symmetry condition $\gamma_{ij} = \gamma_{ji}$. Let $a > 1$ be real , and let $N(Z)$ denote the number of sets of integers $u_1, \ldots, u_{2n}$ (including 0) satisfying

$$\begin{cases} |u_1| < aZ, \ldots, |u_n| < aZ, \\ |L_1 - u_{n+1}| < a^{-1}Z, \ldots, |L_n - u_{2n}| < a^{-1}Z. \end{cases} \tag{12.6}$$

Then, if $0 < Z_1 \le Z_2 \le 1$, we have

$$\frac{N(Z_2)}{N(Z_1)} \ll \left(\frac{Z_2}{Z_1}\right)^n. \tag{12.7}$$

Proof. The inequalities are equivalent to

$$|x_1| < Z, \ldots, |x_n| < Z, \qquad |x_{n+1}| < Z, \ldots, |x_{2n}| < Z$$

for the general point $(x_1, \ldots, x_{2n})$ of the $2n$-dimensional lattice Λ defined above. Hence the inequalities imply that $|\mathbf{x}| < \sqrt{2n}Z$. On the other hand, the inequalities are implied by $|\mathbf{x}| < Z$. Hence if $N_0(Z)$ denotes the number of points of Λ (including the origin) with $|\mathbf{x}| < Z$, we have

$$N_0(Z) \le N(Z) \le N_0(\sqrt{2n}Z).$$

Thus, if $0 < Z_1 \le Z_2 < 1$,

$$\frac{N(Z_2)}{N(Z_1)} \le \frac{N_0(\sqrt{2n}Z_2)}{N_0(Z_1)}.$$

If we prove the result corresponding to (12.7), namely

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \left(\frac{Z_2}{Z_1}\right)^n, \tag{12.8}$$

under the weaker condition $Z_2 \ll 1$ instead of $Z_2 \leq 1$, we can apply it with Z_2 replaced by $\sqrt{2n}Z_2$ and so deduce (12.7).

Let $R_1, \ldots, R_{2n}$ denote the successive minima of Λ. We have seen that

$$R_n \ll 1 \ll R_{n+1}.$$

Define ν and μ by

$$R_\nu \leq Z_1 < R_{\nu+1}, \quad R_\mu \leq Z_2 < R_{\mu+1},$$

so that $\nu \leq \mu$. By Lemma 12.4,

$$N_0(Z_1) \gg \frac{Z_1^\nu}{R_1 \cdots R_\nu} \quad \text{and} \quad N_0(Z_2) \ll \frac{Z_2^\mu}{R_1 \cdots R_\mu},$$

whence

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu}.$$

If $\mu \leq n$, the result (12.8) follows, since the right-hand side is

$$\leq \frac{Z_2^\mu}{Z_1^\mu} \leq \left(\frac{Z_2}{Z_1}\right)^n.$$

If $\mu > n$ and $\nu \leq n$, we write the expression as

$$\frac{Z_2^n}{Z_1^\nu R_{\nu+1} \cdots R_n} \frac{Z_2^{\nu-n}}{R_{n+1} \cdots R_\mu},$$

and since $Z_2 \ll 1$ and $R_{n+1} \gg 1$ the result again follows. Finally, the possibility $\nu > n$ can only arise if $Z_1 \gg 1$, in which case

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu} \ll 1 \ll \left(\frac{Z_2}{Z_1}\right)^n.$$

This proves Lemma 12.6. □

Note. The significance of Lemma 12.6 is that the number of solutions of the inequalities (12.6) does not diminish too rapidly as Z diminishes. The result is of interest only if aZ is large, for if $aZ < 1$ the inequalities imply $u_1 = \cdots = u_{2n} = 0$, and $N(Z) = 1$.

It appears that without the symmetry condition on the coefficients γ_{ij} in the linear forms $L_1, \ldots, L_n$, one could assert only a weaker result in which the exponent n would be replaced by $2n - 1$.